

# COUNTING FIXED POINTS AND TWO-CYCLES OF THE SINGULAR MAP $x \mapsto x^{x^n}$ MODULO POWERS OF A PRIME

JOSHUA HOLDEN, PAMELA A. RICHARDSON, AND MARGARET M. ROBINSON

**ABSTRACT.** The “self-power” map  $x \mapsto x^x$  modulo  $m$  and its generalized form  $x \mapsto x^{x^n}$  modulo  $m$  are of considerable interest for both theoretical reasons and for potential applications to cryptography. In this paper, we use  $p$ -adic methods, primarily  $p$ -adic interpolation, Hensel’s lemma, and lifting singular points modulo  $p$ , to count fixed points and two-cycles of equations related to these maps when  $m$  is a prime power.

## 1. INTRODUCTION

The study of the “self-power” map  $x \mapsto x^x$  modulo  $m$  goes back at least to two papers by Crocker in the 1960’s [9, 10]. Its study has accelerated in recent years due to both improvements in technique (see, for instance, [1–3, 7, 8, 11–13, 15–18, 21, 25]) and its relation to a variation of the ElGamal digital signature scheme given in, e.g., [23, Note 11.71]. In particular, [18] and [24] used  $p$ -adic techniques to investigate solutions to the equations (among others)

$$(1) \quad x^x \equiv c \pmod{p^e}$$

for fixed  $c$  and  $x$  in  $\{1, \dots, p^e(p-1)\}$  and

$$(2) \quad h^h \equiv a^a \pmod{p^e}$$

for  $x$  and  $y$  in  $\{1, \dots, p^e(p-1)\}$ .

In this work we will use similar techniques investigate the number of fixed points of the self-power map, i.e., solutions to

$$(3) \quad x^x \equiv x \pmod{p^e},$$

and two-cycles, or solutions to

$$(4) \quad x^x \equiv y \pmod{p^e} \quad \text{and} \quad y^y \equiv x \pmod{p^e}.$$

In fact, we give results for the more general situations

$$(5) \quad x^{x^n} \equiv x \pmod{p^e}$$

and

$$(6) \quad x^{x^n} \equiv y \pmod{p^e} \quad \text{and} \quad y^{y^n} \equiv x \pmod{p^e}$$

for all  $p$  and  $n$ .

---

2010 *Mathematics Subject Classification.* Primary 11D88; Secondary 11A07, 11T71, 94A60.

*Key words and phrases.* self-power map,  $p$ -adic interpolation, Hensel’s Lemma, singular lifting, fixed points, two-cycles.

The second author would like to thank the Hutchcroft Fund at Mount Holyoke College for support and the Department of Mathematics at Mount Holyoke for their hospitality during a visit in the spring of 2015.

This particular generalization was inspired by study of the map  $x \mapsto g^{x^n}$  modulo  $p$  for a fixed integer  $g$ , which has been used in a secret sharing scheme [26] and a group signature scheme [5], among other places. A preliminary study of the case  $n = 2$  of this map was begun in [28], and the solutions to  $g^{x^n} \equiv x^k$  modulo  $p^e$  were later studied in [22] with some conditions on  $p$ ,  $k$ , and  $n$ . It is also known that the discrete logarithm problem, that is, the problem of inverting the map  $x \mapsto g^x$  modulo  $p$ , can be solved more quickly if a value of  $g^{x^n}$  modulo  $p$  is known in addition. (See [6], for example.) It would be interesting to know if this also applied to the self-power map. For a general polynomial  $g(x)$ , we also give some results on the generalized self-power map  $x \mapsto x^{g(x)}$  in the case  $e = 1$ . Other results for this map, including discussions of fixed points, appear in [21, Thm. 10] and [7, Cor. 2].

The primary  $p$ -adic techniques used in this paper are  $p$ -adic interpolation and lifting techniques, including Hensel's lemma and lifting singular points modulo  $p$ . Section 2 provides the necessary background for these. Section 3 counts the number of fixed points, that is, solutions of (5), for both odd  $p$  and  $p = 2$ . Likewise, Section 4 counts the number of two-cycles, or solutions of (6), for odd and even  $p$ . Finally, Section 5 discusses future work.

## 2. INTERPOLATION AND LIFTING

Let  $p$  be a prime, and let  $q = 4$  if  $p = 2$ ,  $q = p$  otherwise. As in [18], our starting point is the difficulty of interpolating the function  $f(x) = x^{x^n}$ , defined on  $x \in \mathbb{Z}$ , to a function on  $x \in \mathbb{Z}_p$ , the ring of  $p$ -adic integers. An analytic interpolation is only possible if the base of our  $p$ -adic exponentiation is in  $1 + q\mathbb{Z}_p$ . (See for example, [14, Section 4.6], [19, Section 4.6], or [20, Section II.2].)

Therefore, we let  $\mu_{\phi(q)} \subseteq \mathbb{Z}_p^\times$ , the units in  $\mathbb{Z}_p$ , be the set of all  $\phi(q)$ -th roots of unity and consider the Teichmüller character

$$\omega : \mathbb{Z}_p^\times \rightarrow \mu_{\phi(q)},$$

which is a surjective homomorphism. (Throughout this paper,  $\phi(m)$  will refer to the Euler phi function.) It is known that  $\mathbb{Z}_p^\times$  has a canonical decomposition as

$$(7) \quad \mathbb{Z}_p^\times \cong \mu_{\phi(q)} \times (1 + q\mathbb{Z}_p)$$

[14, Cor. 4.5.10], and thus for  $x$  in  $\mathbb{Z}_p^\times$ , we may uniquely write  $x = \omega(x) \langle x \rangle$  for some  $\langle x \rangle \in 1 + q\mathbb{Z}_p$ .

**Proposition 1.** *Let  $x_0 \in \mathbb{Z}/\phi(q)\mathbb{Z}$ , and let*

$$I_{x_0} = \{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{\phi(q)}\} \subseteq \mathbb{Z}.$$

*Let  $g(x)$  be any polynomial. Then*

$$f_{x_0}(x) = \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} = \omega(x)^{g(x_0)} \exp(g(x) \log \langle x \rangle)$$

*defines a function which is analytic on  $1 + q\mathbb{Z}_p$  and locally analytic on  $\mathbb{Z}_p^\times$ , such that  $f_{x_0}(x) = x^{g(x)}$  whenever  $x \in I_{x_0}$ .*

**REMARK 1.** Note that when  $p = 2$ ,  $I_1 = \mathbb{Z} \setminus 2\mathbb{Z}$ , which is dense in  $\mathbb{Z}_2^\times$ . Therefore we will only need one version of  $f_{x_0}(x)$  in this case.

*Proof.* The map  $x \mapsto \langle x \rangle^{g(x)}$  is defined in the obvious way for any  $x \in \mathbb{N} \setminus p\mathbb{N}$ , but for such an  $x$ , we have  $\exp(g(x) \log \langle x \rangle) = \exp(\log(\langle x^{g(x)} \rangle)) = \langle x \rangle^{g(x)}$  by the properties of  $p$ -adic exponential and logarithmic functions. Both versions of

the function are thus uniformly continuous and bounded on  $\mathbb{N} \setminus p\mathbb{N}$  and can be interpolated to  $\mathbb{Z}_p^\times$  by Problem 185 of [14]. Such an interpolation is unique, and thus equality holds on  $\mathbb{Z}_p$ , with both versions having the desired analyticity since  $\exp(g(x) \log \langle x \rangle)$  does. Also  $\omega(x)^{g(x_0)}$  is constant on  $1 + q\mathbb{Z}_p$  and locally constant on  $\mathbb{Z}_p$ , so  $f_{x_0}$  has the desired analyticity.

If  $x \in I_{x_0}$ , then  $g(x_0) \equiv g(x)$  modulo  $\phi(q)$ , so  $\omega(x)^{g(x_0)} = \omega(x)^{g(x)}$ . Thus

$$f_{x_0}(x) = \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} = \omega(x)^{g(x)} \langle x \rangle^{g(x)} = x^{g(x)},$$

as desired.  $\square$

Finally, we will want a version of Hensel's lemma that applies to power series, not just polynomials. We will use this in the cases where the solution to an equation is nonsingular modulo  $p$ .

**DEFINITION 1** (Defn. III.4.2.2 of [4]). A power series  $f(x_1, x_2, \dots, x_n)$  in the ring of formal power series  $\mathbb{Z}_p[[x_1, \dots, x_n]]$  with coefficients in  $\mathbb{Z}_p$  is called *restricted* if  $f(x_1, \dots, x_n) = \sum_{(\alpha_i)} C_{\alpha_1, \alpha_2, \dots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  and for every neighborhood  $V$  of 0 in  $\mathbb{Z}_p$  there is only a finite number of coefficients  $C_{\alpha_1, \alpha_2, \dots, \alpha_n}$  not belonging to  $V$  (in other words, the family  $(C_{\alpha_1, \alpha_2, \dots, \alpha_n})$  tends to 0 in  $\mathbb{Z}_p$ ).

In particular, the series in this paper are going to be  $p$ -adic convergent series  $\sum_{\alpha} C_{\alpha} x^{\alpha}$  in  $\mathbb{Z}_p[[x]]$  such that  $\lim_{\alpha \rightarrow \infty} |C_{\alpha}|_p = 0$ .

**DEFINITION 2.** Let  $f(x)$  be a restricted power series in  $\mathbb{Z}_p[[x]]$ . A point  $a$  in  $\mathbb{Z}_p$  is called *nonsingular modulo  $p$*  if  $\frac{df}{dx}(a)$  is in  $\mathbb{Z}_p^\times$ . Otherwise,  $\frac{df}{dx}(a) \equiv 0 \pmod{p}$  and the point  $a$  is called *a singular point modulo  $p$* .

**Proposition 2** (See Cor. III.4.5.2 of [4]). *Let  $f(x)$  be a restricted power series in  $\mathbb{Z}_p[[x]]$ , and let  $a$  be in  $\mathbb{Z}_p$  such that  $\frac{df}{dx}(a)$  is in  $\mathbb{Z}_p^\times$  and  $f(a) \equiv 0 \pmod{p}$ . Then there exists a unique  $x \in \mathbb{Z}_p$  for which  $x \equiv a \pmod{p}$  and  $f(x) = 0$  in  $\mathbb{Z}_p$ .*

### 3. FIXED POINTS

In this section, we are concerned with counting roots  $x$  of the function  $x^{x^n} - x \pmod{p^e}$ , where for a positive integer  $e$  and a prime  $p$ , we allow  $x \in \{1, 2, \dots, p^e(p-1)\}$  such that  $p \nmid x$ . To begin, we fix  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$  and consider an auxiliary function  $\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x \pmod{p^e}$  defined for any polynomial  $g(x)$ .

**Theorem 3.** *Let  $p$  be a prime  $p \neq 2$  and  $g(x)$  be a polynomial. Then for every  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , there are  $\gcd(p-1, g(x_0)-1)$  solutions  $x$  to the congruence*

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$$

where  $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ . Alternatively, for any given  $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ , there are

$$N_{g-1}(\text{ord}_p x) \frac{p-1}{\text{ord}_p x}$$

values of  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$  such that

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p},$$

where  $N_{g-1}(d)$  is the number of solutions to  $g(z) - 1 \equiv 0$  modulo  $d$  and  $\text{ord}_p x$  is the multiplicative order of  $x$  modulo  $p$ .

*Proof.* We know that  $\langle x \rangle \equiv 1 \pmod{p}$ , so the congruence reduces to

$$(8) \quad \omega(x)^{g(x_0)} \equiv x \pmod{p}.$$

For fixed  $x_0$ , since  $\omega(x) \equiv x \pmod{p}$  by definition, equation (8) has a solution if and only if

$$\omega(x)^{g(x_0)-1} \equiv 1 \pmod{p}.$$

This congruence is satisfied for exactly the  $x \in (\mathbb{Z}/p\mathbb{Z})^\times$  for which  $\text{ord}_p(x)$  divides  $g(x_0) - 1$ . There will be  $\gcd(p-1, g(x_0) - 1)$  such values for  $x$  in the cyclic group  $(\mathbb{Z}/p\mathbb{Z})^\times$ .

On the other hand, if  $x$  is fixed, then  $\text{ord}_p(x)$  divides  $g(x_0) - 1$  if and only if  $g(x_0) - 1 \equiv 0 \pmod{\text{ord}_p(x)}$ . There are  $N_{g-1}(\text{ord}_p x)$  such values of  $x_0$  in  $\mathbb{Z}/(\text{ord}_p x)\mathbb{Z}$  and  $N_{g-1}(\text{ord}_p x)(p-1)/\text{ord}_p x$  such values of  $x_0$  in  $\mathbb{Z}/(p-1)\mathbb{Z}$ .  $\square$

Next we use the Chinese Remainder Theorem to get the following corollary to Theorem 3.

**Corollary 4.** *Let  $p$  be a prime,  $p \neq 2$ . Then there are*

$$\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0) - 1) = \sum_{d|p-1} \phi(d)((p-1)/d)N_{g-1}(d)$$

*solutions  $x$  to the congruence*

$$x^{g(x)} \equiv x \pmod{p}$$

*where  $1 \leq x \leq p(p-1)$  and  $p \nmid x$ .*

*Proof.* Theorem 3 implies that for each choice of  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , there are  $\gcd(p-1, g(x_0) - 1)$  elements  $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  with the property that

$$\omega(x_1)^{g(x_0)} \langle x_1 \rangle^{g(x_1)} \equiv x_1 \pmod{p}.$$

By the Chinese Remainder Theorem, there will be exactly one  $x \in \mathbb{Z}/p(p-1)\mathbb{Z}$  such that  $x \equiv x_0 \pmod{p-1}$  and  $x \equiv x_1 \pmod{p}$ . By the interpolation we set up in the introduction, since  $x \equiv x_0 \pmod{p-1}$ , we know that for each such  $x$ :

$$x^{g(x)} = \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv \omega(x_1)^{g(x_0)} \langle x_1 \rangle^{g(x_1)} \equiv x_1 \equiv x \pmod{p}.$$

Finally, since exactly  $\gcd(p-1, g(x_0) - 1)$  such  $x$  exist for each  $x_0$ , we have  $\sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0) - 1)$  solutions to the congruence.

Alternatively, for each choice of  $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  of multiplicative order  $d$  modulo  $p$ , there are  $((p-1)/d)N_{g-1}(d)$  values of  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$  satisfying the congruence and  $\phi(d)$  choices of  $x_1$  with multiplicative order  $d$  for each  $d \mid (p-1)$ . (The equality of the two sums also follows from [27, Theorem 1]).  $\square$

Next we consider  $p$ -adic solutions to our equation for  $x$  such that  $g(x) \not\equiv 1 \pmod{p}$ . These are the cases where the solutions are nonsingular modulo  $p$  and thus lift uniquely.

**Theorem 5.** *Let  $p$  be a prime,  $p \neq 2$ . Then there are*

$$\left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, g(x_0) - 1) \right\} - \left\{ \sum_{g(x_1) \equiv 1 \pmod{p}} N_{g-1}(\text{ord}_p(x_1)) \frac{p-1}{\text{ord}_p(x_1)} \right\}$$

$$= \sum_{d|p-1} |\{x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times \mid g(x_1) \not\equiv 1 \pmod{p}, \text{ord}_p(x_1) = d\}| \frac{p-1}{d} N_{g-1}(d)$$

solutions  $x$  to the congruence

$$(9) \quad x^{g(x)} \equiv x \pmod{p^e}$$

where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$  and  $g(x) \not\equiv 1 \pmod{p}$ .

*Proof.* For the cases where  $g(x_1) \equiv 1 \pmod{p}$ ,  $x_1^{g(x_1)-1} \equiv 1 \pmod{p}$  for all  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$  such that  $\text{ord}_p(x_1) \mid (g(x_0) - 1)$ . There will be  $N_{g-1}(\text{ord}_p(x_1))(p-1)/\text{ord}_p(x_1)$  such values of  $x_0$ . Now by the Chinese Remainder Theorem, there will be  $N_{g-1}(\text{ord}_p(x_1))(p-1)/\text{ord}_p(x_1)$  values for  $x$  with  $1 \leq x \leq p(p-1)$  where  $p \nmid x$  and  $g(x) \equiv 1 \pmod{p}$ .

Now we have left to show that for a fixed  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , any solution with  $g(x_1) \not\equiv 1 \pmod{p}$  to the equation

$$\omega(x)^{g(x_0)} \langle x \rangle^{x^{g(x)}} \equiv x \pmod{p}$$

will lift to a unique solution in  $\mathbb{Z}_p$ . This result will imply by the Chinese Remainder Theorem that the number of solutions to  $x^{g(x)} \equiv x \pmod{p^e}$ , where we allow  $x \in \{1, 2, \dots, p^e(p-1)\}$  such that  $p \nmid x$  and  $g(x) \not\equiv 1 \pmod{p}$ , will be exactly the number of solutions when  $e = 1$ .

Fix  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , and consider the function  $f_{x_0} : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  given by  $f_{x_0}(x) = \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x$ . Note that

$$\begin{aligned} f_{x_0}(x) &= \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x \\ &= \omega(x)^{g(x_0)} (\exp(g(x) \log \langle x \rangle)) - x \\ &= \omega(x)^{g(x_0)} \left( 1 + g(x) \log \langle x \rangle + \frac{g(x)^2 (\log \langle x \rangle)^2}{2!} + \dots \right) - x. \end{aligned}$$

Now  $\log \langle x \rangle \in p\mathbb{Z}_p$ , so

$$\begin{aligned} f'_{x_0}(x) &= \omega(x)^{g(x_0)} ((g'(x_0) \log \langle x \rangle + g(x)/x) + (\text{terms containing } p)) - 1 \\ f'_{x_0}(x) &\equiv \omega(x)^{g(x_0)} g(x)/x - 1 \pmod{p} \\ &\equiv x^{g(x_0)-1} g(x) - 1 \pmod{p} \quad (\text{since } \omega(x) \equiv x \pmod{p}). \end{aligned}$$

Suppose we have an  $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  such that  $g(x_1) \not\equiv 1 \pmod{p}$  and  $\omega(x_1)^{g(x_0)} \langle x_1 \rangle^{g(x_1)} \equiv x_1 \pmod{p}$ . Again, since  $\omega(x_1) \equiv x_1 \pmod{p}$  and  $\langle x_1 \rangle \equiv 1 \pmod{p}$ , this gives us  $x_1^{g(x_0)} \equiv x_1 \pmod{p}$ . Hence,

$$\begin{aligned} f'_{x_0}(x_1) &\equiv x_1^{g(x_0)-1} g(x_1) - 1 \pmod{p} \\ &\equiv g(x_1) - 1 \pmod{p}. \end{aligned}$$

Since  $g(x_1) \not\equiv 1 \pmod{p}$ , we have that  $f'_{x_0}(x_1) \not\equiv 0 \pmod{p}$ .

By Proposition 2, for fixed  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , each solution  $x_1$  with  $g(x_1) \not\equiv 1 \pmod{p}$  to the equation

$$\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv x \pmod{p}$$

will lift to a unique solution to  $\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - x$  in  $\mathbb{Z}_p$ . Thus this unique solution in  $\mathbb{Z}_p$  will correspond to one solution to equation (9) for each  $e$ . Putting these results together with Corollary 4 and taking out the solutions where  $g(x) \equiv 1 \pmod{p}$ , we have our theorem.

The second summation follows by noting that for each choice of  $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  of multiplicative order  $d$  modulo  $p$  such that  $g(x_1) \not\equiv 1$  modulo  $p$ , there are  $((p-1)/d)N_{g^{-1}}(d)$  values of  $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$  satisfying the congruence.  $\square$

**Corollary 6.** *Let  $p$  be a prime  $p \neq 2$ , then there are*

$$\begin{aligned} & \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, x_0^n - 1) \right\} - \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, n, x_0^n - 1) \right\} \\ &= \left\{ \sum_{d|p-1} \phi(d) \frac{p-1}{d} N_{x^n-1}(d) \right\} - \left\{ \sum_{d|\gcd(n, p-1)} \phi(d) \frac{p-1}{d} N_{x^n-1}(d) \right\} \end{aligned}$$

*solutions  $x$  to the congruence*

$$(10) \quad x^{x^n} \equiv x \pmod{p^e}$$

*where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$  and  $x^n \not\equiv 1 \pmod{p}$ .*

*In particular, there are*

$$\begin{aligned} & \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, x_0 - 1) \right\} - (p-1) \\ &= \left\{ \sum_{d|p-1} \phi(d) \frac{p-1}{d} \right\} - \left\{ \sum_{d|\gcd(n, p-1)} \phi(d) \frac{p-1}{d} \right\} \end{aligned}$$

*solutions  $x$  to the congruence*

$$(11) \quad x^x \equiv x \pmod{p^e}$$

*where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$  and  $x \not\equiv 1 \pmod{p}$ .*

*Proof.* Let  $g(x) = x^n$ . Then for each choice of  $x_0$  in Theorem 3, there are  $\gcd(p-1, n, x_0^n - 1)$  elements  $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  with the property that both  $\omega(x)^{x_0^n - 1} \equiv 1 \pmod{p}$  and  $g(x) = x^n \equiv 1 \pmod{p}$ , since  $\omega(x) \equiv x \pmod{p}$ , and thus these are together equivalent to

$$\omega(x)^{\gcd(n, x_0^n - 1)} \equiv 1 \pmod{p}.$$

On the other hand,  $g(x) \equiv 1$  modulo  $p$  is equivalent to  $\text{ord}_p(x) \mid n$ , which is equivalent to  $\text{ord}_p(x) \mid \gcd(n, p-1)$ . So in the previous theorem,

$$\left| \{x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times \mid g(x_1) \not\equiv 1 \pmod{p}, \text{ord}_p(x_1) = d\} \right| = \phi(d)$$

if  $d$  divides  $p-1$  but not  $\gcd(n, p-1)$  and 0 otherwise.  $\square$

Now we need to specialize to  $g(x) = x^n$  in order to look at the solutions that are singular modulo  $p$ .

**DEFINITION 3.** Let  $G_{a,e}$  equal the set of solutions  $x$  to the equation

$$x^{x^n} \equiv x \pmod{p^e}$$

where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$  and  $x \equiv a \pmod{q}$ . Recall that  $q = p$  when  $p$  is odd, and  $q = 4$  when  $p = 2$ .

**Theorem 7.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \nmid n$ , and  $\xi \in \mathbb{Z}_p$  be an  $n$ th root of unity. Then*

$$|G_{\xi,e}| = \frac{p-1}{\text{ord}_p(\xi)} N_{x^n-1}(\text{ord}_p(\xi)) \cdot p^{\lfloor e/2 \rfloor}.$$

*Proof.* Consider  $x \equiv \xi$  modulo  $p$ . Let  $0 \leq x_0 \leq p-1$ , and let  $f_{x_0}(x) = \omega(x)^{x_0^n} \langle x \rangle^{x^n} - x$ . Since we are assuming  $\xi$  is a root of unity, we have that  $\omega(x) = \xi$ . We noted in the proof of Theorem 3 that if  $\text{ord}_p(\xi) = \text{ord}_p(x)$  does not divide  $x_0^n - 1$ , then there are no solutions to  $f_{x_0}(x) \equiv 0$  modulo  $p$  and thus no solutions to  $f_{x_0}(x) \equiv 0 \pmod{p^e}$  for any positive integer  $e$ . Thus, we assume that  $\text{ord}_p(\xi)$  divides  $x_0^n - 1$ , so  $\omega(x)^{x_0^n} = \xi^{x_0^n} = \xi$ . Then we have that

$$(12) \quad f_{x_0}(x) = \xi \langle x \rangle^{x^n} - x = \xi \exp(x^n \log \langle x \rangle) - x.$$

Also, note that

$$f'_{x_0}(x) = \xi \exp(x^n \log \langle x \rangle) (nx^{n-1} \log \langle x \rangle + x^{n-1}) - 1$$

and

$$f''_{x_0}(x) = \xi \exp(x^n \log \langle x \rangle) ((nx^{n-1} \log \langle x \rangle + x^{n-1})^2 + n(n-1)x^{n-2} \log \langle x \rangle + (2n-1)x^{n-2}).$$

Since  $\xi^n = 1$  and  $\langle \xi \rangle = 1$ , we have  $f_{x_0}(\xi) = 0$ ,  $f'_{x_0}(\xi) = 0$ , and  $f''_{x_0}(\xi) = \xi^{2n-1} + (2n-1)\xi^{n-1} = 2n\xi^{-1}$ .

The Taylor series expansion for  $f_{x_0}(x)$  centered at  $x = \xi$  is therefore

$$\begin{aligned} f_{x_0}(x) &= f_{x_0}(\xi) + f'_{x_0}(\xi)(x - \xi) + \frac{f''_{x_0}(\xi)}{2!}(x - \xi)^2 \\ &\quad + (\text{higher powers of } (x - \xi)) \\ &= 0 + 0(x - \xi) + n\xi^{-1}(x - \xi)^2 + (\text{higher powers of } (x - \xi)) \\ &= n\xi^{-1}(x - \xi)^2 + (\text{higher powers of } (x - \xi)). \end{aligned}$$

We proceed by induction on  $e$  to count the number of solutions  $x$  to  $f_{x_0}(x) \equiv 0$  modulo  $p^e$  such that  $x \equiv \xi$  modulo  $p$ . When  $e = 1$ , there is only one  $x \equiv \xi$  modulo  $p$ , and by the above Taylor series expansion,  $f_{x_0}(x) \equiv 0$  modulo  $p$ .

Now consider a solution  $x$  modulo  $p^e$ ; we want to know how many solutions it lifts to modulo  $p^{e+1}$ . Each solution looks like  $x + tp^e$  for some  $0 \leq t < p$ . Modulo  $p^{e+1}$ ,  $f_{x_0}(x + tp^e) \equiv f_{x_0}(x) + tp^e f'_{x_0}(x)$  by Taylor series expansion around  $x$ . We are assuming  $f_{x_0}(x) \equiv 0$  modulo  $p^e$ , so we can divide through by  $p^e$ . Then  $f_{x_0}(x + tp^e) \equiv 0$  modulo  $p^{e+1}$  if and only if  $tf'_{x_0}(x) \equiv f_{x_0}(x)/p^e$  modulo  $p$ . We saw that  $f'_{x_0}(x) \equiv 0$  modulo  $p$ , so that there are either  $p$  solutions, if  $f_{x_0}(x)/p^e \equiv 0$  modulo  $p$ , or no solutions if not.

For  $z \in \mathbb{Z}_p$ , let  $v_p(z)$  be the  $p$ -adic valuation of  $z$ . Then, using the Taylor expansion above and the assumption that  $p \nmid n$ ,  $v_p(f_{x_0}(x)) = 2v_p(x - \xi)$ . We assumed  $f_{x_0}(x) \equiv 0$  modulo  $p^e$ , so that's equivalent to  $2v_p(x - \xi) \geq e$ .

Suppose  $e$  is odd, so  $e = 2k - 1$  for some positive integer  $k$ . Then  $2v_p(x - \xi) \geq 2k - 1$  implies  $v_p(x - \xi) \geq k$ , or  $v_p(f_{x_0}(x)) \geq 2k = e + 1$ . Thus  $p^{e+1} \mid f_{x_0}(x)$ , and  $x$  lifts to  $p$  solutions modulo  $p^{e+1}$ .

Now suppose  $e$  is even, so  $e = 2k$  for some positive integer  $k$ . By the preceding argument,  $v_p(f_{x_0}(x)) \geq e = 2k$  if and only if  $v_p(x - \xi) \geq k$ , and  $v_p(f_{x_0}(x)) \geq e + 1 = 2k + 1$  if and only if  $v_p(x - \xi) \geq k + 1$ . We are assuming  $v_p(f_{x_0}(x)) \geq e$ , which thus is equivalent to  $x = \xi + a_k p^k + \alpha p^{k+1}$  for some  $0 \leq a_k \leq p - 1$  and  $\alpha$  in

$\mathbb{Z}_p$ . Thus  $v_p(x - \xi) \geq k + 1$  if and only if  $a_k = 0$ , and  $x$  lifts to exactly one solution modulo  $p^e$ .

Since we are looking for solutions to  $x^{x^n} - x \equiv 0 \pmod{p^e}$  where  $1 \leq x \leq p^e(p-1)$  and  $x \equiv \xi \pmod{p}$ , we must use the Chinese Remainder Theorem to argue that for each of the  $[(p-1)/\text{ord}_p(\xi)]N_{x^n-1}(\text{ord}_p(\xi))$  values of  $x_0$  for which  $1 \leq x_0 \leq p-1$  and  $\text{ord}_p(\xi) \mid x_0^n - 1$ , and for each of the  $p^{\lfloor e/2 \rfloor}$  solutions  $x_1$  to  $\omega(x)^{x_0^n} x^{x^n} - x \pmod{p^e}$  where  $1 \leq x_1 \leq p^e$  and  $x_1 \equiv \xi \pmod{p}$ , there will be exactly one such  $x$  where  $1 \leq x \leq p^e(p-1)$  and  $x \equiv \xi \pmod{p}$ . Hence,  $|G_{\xi,e}| = \frac{(p-1)}{\text{ord}_p(\xi)} N_{x^n-1}(\text{ord}_p(\xi)) \cdot p^{\lfloor e/2 \rfloor}$ .  $\square$

Now combining our results from Corollary 6 and Theorem 7, we have the following theorem for  $p \neq 2$  and  $p \nmid n$ .

**Theorem 8.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \nmid n$ , then there are*

$$\begin{aligned} & \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, x_0^n - 1) \right\} + \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, n, x_0^n - 1) \cdot (p^{\lfloor e/2 \rfloor} - 1) \right\} \\ = & \left\{ \sum_{d|p-1} \phi(d) \left( \frac{p-1}{d} \right) N_{x^n-1}(d) \right\} + \left\{ \sum_{d|\gcd(n, p-1)} \phi(d) \left( \frac{p-1}{d} \right) N_{x^n-1}(d) \cdot (p^{\lfloor e/2 \rfloor} - 1) \right\} \end{aligned}$$

*solutions  $x$  to the congruence*

$$x^{x^n} \equiv x \pmod{p^e}$$

*where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$ .*

*In particular, there are*

$$\begin{aligned} & \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, x_0 - 1) \right\} + (p-1) (p^{\lfloor e/2 \rfloor} - 1) \\ = & \left\{ \sum_{d|p-1} \phi(d) \left( \frac{p-1}{d} \right) \right\} + (p-1) (p^{\lfloor e/2 \rfloor} - 1) \end{aligned}$$

*solutions  $x$  to the congruence*

$$x^x \equiv x \pmod{p^e}$$

*where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$ .*

*Proof.* This follows directly from Corollary 6 and Theorem 7. (Note that there are  $\gcd(p-1, n)$  elements of  $\mathbb{Z}_p$  which are  $n$ th roots of unity, and each of them is congruent to a unique integer modulo  $p$ .)  $\square$

If  $p \mid n$ , the lifting for solutions that are singular modulo  $p$  works the same for large  $e$  as in Theorem 7, but for small  $e$ , all solutions lift.

**Theorem 9.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \mid n$ , and  $\xi \in \mathbb{Z}_p$  be an  $n$ th root of unity. Then*

$$|G_{\xi,e}| = \frac{p-1}{\text{ord}_p(\xi)} N_{x^n-1}(\text{ord}_p(\xi)) \cdot \begin{cases} p^{e-1} & \text{if } e \leq v_p(n) \\ p^{\lfloor (e+v_p(n))/2 \rfloor} & \text{if } e \geq v_p(n) + 1 \end{cases}$$

REMARK 2. Note that in fact the two formulas are equal if  $e = v_p(n) + 1$  or  $e = v_p(n) + 2$ .



*Proof.* As in the proof of Theorem 7, consider  $x \equiv \xi$  modulo  $p$ , let  $0 \leq x_0 \leq p-1$ , and let  $f_{x_0}(x) = \omega(x)^{x_0^n} \langle x \rangle^{x^n} - x$ . Once again we assume that  $\text{ord}_p(\xi)$  divides  $x_0^n - 1$  and we have  $f_{x_0}(\xi) = 0$ ,  $f'_{x_0}(\xi) = 0$ , and  $f''_{x_0}(\xi) = 2n\xi^{-1}$ . Note that since  $f''_{x_0}(x)$  is of the form  $nU(x) + (x^n - 1)V(x)$ , an induction shows that  $f^{(i)}(x)$  is of the same form for every  $i \geq 2$ , and thus  $f^{(i)}(\xi)$  is divisible by  $n$  for every  $i \geq 2$ . Thus the Taylor series expansion for  $f_{x_0}(x)$  centered at  $x = \xi$  is

$$f_{x_0}(x) = n\xi^{-1}(x - \xi)^2 + n(\text{higher powers of } (x - \xi)).$$

Thus  $v_p(f_{x_0}(x)) = v_p(n\xi^{-1}(x - \xi)^2) = 2v_p(x - \xi) + v_p(n)$ .

Let  $\ell = v_p(n)$ . If  $1 \leq e \leq \ell + 2$ , note that for all  $x$  such that  $1 \leq x \leq p^e$  and  $x \equiv \xi \pmod{p}$ ,  $v_p(f_{x_0}(x)) \geq 2 + \ell \geq e$ , so  $f_{x_0}(x) \equiv 0 \pmod{p^e}$ . There are  $p^{e-1}$  such values of  $x$ , so there are  $p^{e-1}$  solutions to  $f_{x_0}(x) \equiv 0 \pmod{p^e}$  for every solution  $\xi$  modulo  $p$ .

Now we induct on  $e$ , using  $e = \ell + 1$  as the base case. We already showed that there are  $p^\ell$  solutions to  $f_{x_0}(x) \equiv 0 \pmod{p^{\ell+1}}$ , and  $p^\ell = p^{\lfloor (\ell+1+\ell)/2 \rfloor}$ , so the base case agrees with the formula.

Assume by way of induction that  $f_{x_0}(x) \equiv 0$  modulo  $p^e$ , so  $2v_p(x - \xi) + \ell \geq e$ , i.e.,  $2v_p(x - \xi) \geq e - \ell$ . The rest of the induction proceeds as in Theorem 7, considering cases when  $e - \ell$  is odd and when  $e - \ell$  is even.

Combining the lifting for  $e \geq \ell + 1$  with the base case gives  $p^{\lfloor (e-\ell)/2 \rfloor}$  solutions modulo  $p^e$  for every solution modulo  $p^{\ell+1}$  and thus  $p^{\lfloor (e-\ell)/2 \rfloor} p^\ell = p^{\lfloor (e+\ell)/2 \rfloor}$  solutions modulo  $p^e$  for each solution modulo  $p$ . Applying the Chinese Remainder Theorem as in Theorem 7 then gives us the result.  $\square$

The following theorem is now parallel to Theorem 8.

**Theorem 10.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \mid n$ . If  $e \leq v_p(n)$ , then there are*

$$\begin{aligned} & \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, x_0^n - 1) \right\} + \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, n, x_0^n - 1) \cdot (p^{e-1} - 1) \right\} \\ &= \left\{ \sum_{d \mid p-1} \phi(d) \left( \frac{p-1}{d} \right) N_{x^n-1}(d) \right\} + \left\{ \sum_{d \mid \gcd(n, p-1)} \phi(d) \left( \frac{p-1}{d} \right) N_{x^n-1}(d) \cdot (p^{e-1} - 1) \right\} \end{aligned}$$

*solutions  $x$  to the congruence*

$$x^{x^n} \equiv x \pmod{p^e}$$

*where  $1 \leq x \leq p^e(p-1)$  such that  $p \nmid x$ . If  $e \geq v_p(n) + 1$ , then there are*

$$\begin{aligned} & \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, x_0^n - 1) \right\} + \left\{ \sum_{x_0=1}^{p-1} \gcd(p-1, n, x_0^n - 1) \cdot (p^{\lfloor (e+v_p(n))/2 \rfloor} - 1) \right\} \\ &= \left\{ \sum_{d \mid p-1} \phi(d) \left( \frac{p-1}{d} \right) N_{x^n-1}(d) \right\} + \left\{ \sum_{d \mid \gcd(n, p-1)} \phi(d) \left( \frac{p-1}{d} \right) N_{x^n-1}(d) \cdot (p^{\lfloor (e+v_p(n))/2 \rfloor} - 1) \right\} \end{aligned}$$

*solutions to the same congruence.*

When  $p = 2$ , we will see that  $f(x) = x^{x^n} - x$  is singular modulo  $p$  for all odd values of  $x$  where  $1 \leq x \leq p^e$ . The following theorem is analogous to Theorem 7 for  $p \nmid n$  and to Theorem 9 for  $p \mid n$  when  $p = 2$ .

**Theorem 11.** *Let  $p = 2$ ,  $\xi = \pm 1$ , and  $n$  be a positive integer. If  $n$  is even, we have that*

$$|G_{\xi,e}| = \begin{cases} p^{e-2} & \text{if } 2 \leq e \leq 4 + v_p(n) \\ p^{\lfloor (e+v_p(n))/2 \rfloor} & \text{if } e \geq 5 + v_p(n) \end{cases}$$

for all  $e \geq 2$ .

If  $n$  is odd, we have that

$$|G_{1,e}| = \begin{cases} p^{e-2} & \text{if } 2 \leq e \leq 4 \\ p^{\lfloor e/2 \rfloor} & \text{if } e \geq 5 \end{cases}, \quad |G_{-1,e}| = \begin{cases} p^{e-2} & \text{if } 2 \leq e \leq 3 \\ p & \text{if } e \geq 4 \end{cases}$$

for all  $e \geq 2$ .

REMARK 3. Note that in fact for even  $n$  when  $\xi = \pm 1$  and for odd  $n$  when  $\xi = 1$ , the formulas for  $|G_{\xi,e}|$  in the two cases are equal if  $e = v_p(n) + 3$  or  $e = v_p(n) + 4$ . When  $n$  is odd and  $\xi = -1$ , the two cases are equal if  $e = 3$ .

*Proof.* Let  $p = 2$ . We want to count the number of solutions to  $f(x) = x^{x^n} - x \pmod{p^e}$  for odd values of  $x$  where  $1 \leq x \leq p^e$ . Because  $\exp(x)$  for  $p = 2$  is only defined on  $1 + q\mathbb{Z}_p$  and we are only interested in  $x$  values that are odd, we can count solutions for  $x \equiv 1 \pmod{q}$  and  $x \equiv -1 \pmod{q}$  separately. (Recall that  $q = 4$  when  $p = 2$ .) Let  $\xi = \pm 1$ , and set  $f(x) = \xi \langle x \rangle^{x^n} - x = \xi \exp(x^n \log \langle x \rangle) - x$ . Note that  $f(x)$  has the same form as  $f_{x_0}$  in (12) in Theorem 7, so the Taylor series for  $f(x)$  centered at  $\xi$  is

$$f(x) = 0 + (\xi^n - 1)(x - \xi) + \frac{1}{2!}(\xi^{2n-1} + (2n-1)\xi^{n-1})(x - \xi)^2 + (\text{higher powers of } (x - \xi)).$$

If  $\xi = 1$ , the Taylor series reduces to

$$f(x) = n(x - \xi)^2 + (\text{higher powers of } (x - \xi))$$

for any  $n$ . If  $\xi = -1$  and  $n$  is even, the Taylor series is

$$f(x) = -n(x - \xi)^2 + (\text{higher powers of } (x - \xi)).$$

Finally, if  $\xi = -1$  and  $n$  is odd, the Taylor series is

$$f(x) = -2(x - \xi) + (n-1)(x - \xi)^2 + (\text{higher powers of } (x - \xi)).$$

Thus we see that  $f(x)$  is singular modulo  $p$  for all odd  $x$  where  $1 \leq x \leq p^e$  and all  $n$ .

Now consider a solution  $x$  to  $f(x) \equiv 0 \pmod{p^e}$ . The same argument used in Theorem 7 shows that there are either  $p$  ways to lift  $x$  modulo  $p^{e+1}$ , if  $f(x)/p^e \equiv 0 \pmod{p}$ , or no lifts otherwise.

Let  $x \equiv \xi \pmod{q}$ . If  $\xi = 1$ , then for all  $n$ , we use the Taylor expansion around  $\xi = 1$  to evaluate  $f(x)$ , and we have that  $v_p(f(x)) = 2v_p(x - \xi) + v_p(n)$ . We assumed  $f(x) \equiv 0 \pmod{p^e}$ , so that is equivalent to  $2v_p(x - \xi) + v_p(n) \geq e$ .

Similarly, if  $\xi = -1$  and  $n$  is even, we use the Taylor expansion around  $\xi = -1$  to evaluate  $f(x)$ , and we have that  $v_p(f(x)) = 2v_p(x - \xi) + v_p(n)$ . We assumed  $f(x) \equiv 0 \pmod{p^e}$ , so that is also equivalent to  $2v_p(x - \xi) + v_p(n) \geq e$ .

However, if  $\xi = -1$  and  $n$  is odd, we use the Taylor expansion around  $\xi = -1$  to evaluate  $f(x)$ , and we have that  $v_p(f(x)) = v_p(x - \xi) + 1$ . We assumed  $f(x) \equiv 0 \pmod{p^e}$ , so that is equivalent to  $v_p(x - \xi) + 1 \geq e$ .

First, assume either that  $n$  is even and  $\xi = \pm 1$  or that  $n$  is odd and  $\xi = 1$ . Let  $v_p(n) = \ell$ ,  $2 \leq e \leq 4 + \ell$ ,  $1 \leq x \leq p^e$ , and  $p \nmid x$ . In this case, since  $x \equiv \xi \pmod{q}$ ,

we have that  $v_p(x - \xi) \geq 2$ , and from the Taylor expansion around  $\xi$ , we have that  $v_p(f(x)) = 2v_p(x - \xi) + v_p(n) \geq 4 + \ell \geq e$  for all odd  $x$  where  $1 \leq x \leq p^e$ . So for  $2 \leq e \leq 4 + \ell$ , there are  $p^{e-2}$  solutions to the equation  $f(x) \equiv 0 \pmod{p^e}$  since there are exactly that many odd  $x$  values modulo  $p^e$  such that  $x \equiv \xi \pmod{q}$ . Note that in the case that  $n$  is odd and  $\xi = 1$ , when  $e = 4$ , the number of solutions can be written  $p^{e-2}$  or  $p^{\lfloor e/2 \rfloor}$ .

We proceed by induction on  $e$  using  $e = 4 + \ell$  as our base case. For  $e \geq 5 + \ell$ , we want to show that  $|G_{\xi, e}| = p^{\lfloor (e+\ell)/2 \rfloor}$ . If  $e = 4 + \ell$ , we know from above that the number of solutions  $p^{e-2} = p^{4+\ell-2} = p^{2+\ell} = p^{\lfloor (e+\ell)/2 \rfloor}$ . Thus, our formula holds for the base case.

Now consider  $e \geq 4 + \ell$ , and assume by way of induction that there are  $p^{\lfloor (e+\ell)/2 \rfloor}$  odd values for  $x$  such that  $f(x) \equiv 0 \pmod{p^e}$  or  $2v_p(x - \xi) + \ell \geq e$ . For any of these solutions  $x$  modulo  $p^e$ , we thus have that  $2v_p(x - \xi) \geq e - \ell$ . The induction then follows as in Theorem 7, considering the cases when  $e - \ell$  is odd and when  $e - \ell$  is even. We have that for  $e \geq 4 + \ell$ , there are  $p^{\lfloor (e+\ell)/2 \rfloor}$  solutions when  $n$  is even and  $\xi = \pm 1$  or when  $n$  is odd and  $\xi = 1$ .

Next, assume  $\xi = -1$  and  $n$  is odd. Then from the Taylor series in powers of  $(x - \xi)$ , we have  $v_p(f(x)) = v_p(x - \xi) + 1$ . Since  $n$  is odd and  $x \equiv \xi \pmod{q}$  for  $2 \leq e \leq 3$  and for  $x$  odd and  $1 \leq x \leq p^e$ , we have that  $v_p(x - \xi) \geq 2$  and  $v_p(f(x)) \geq 3 \geq e$ . Since there are  $p^{e-2}$  such  $x \equiv \xi \pmod{q}$ , they are all solutions to  $f(x) \equiv 0 \pmod{p^e}$ .

We proceed by induction on  $e$ , using  $e = 3$  as our base case. We need to show by induction that for all  $e \geq 3$ ,  $|G_{-1, e}| = p$ . If  $e = 3$ , we showed above that  $|G_{-1, 3}| = p^{e-2} = p$ , so our formula holds in the base case. Now for  $e \geq 3$ , we need to show that  $|G_{-1, e+1}| = |G_{-1, e}| = p$ .

Suppose that  $x$  is a solution modulo  $p^e$  for  $e \geq 3$ . By induction, we know there will be two (i.e.,  $p$ ) such solutions. We have that  $v_p(x - \xi) \geq e - 1$ . Thus,  $p^{e+1} \mid f(x)$  if and only if  $v_p(x - \xi) \geq e$ , and so  $x = \xi + a_{e-1}p^{e-1} + a_ep^e + \alpha p^{e+1}$  for  $a_{e-1} \in \{0, 1\}$  will be a solution modulo  $p^{e+1}$  if and only if  $a_{e-1} = 0$ . Thus only one of the solutions modulo  $p^e$  ( $x \equiv -1 \pmod{p^e}$ ) will lift to a solution modulo  $p^{e+1}$ , and it will lift to the two possible solutions where  $a_e = 0, 1$ . We have shown by induction that  $|G_{-1, e+1}| = |G_{-1, e}| = p$ . Thus,  $|G_{-1, e}| = p$  for all  $e \geq 3$ .

This concludes the proof of our theorem.  $\square$

**Corollary 12.** *If  $p = 2$  and  $n$  is a positive integer, then the number of solutions to the congruence*

$$x^{x^n} \equiv x \pmod{p^e}$$

*where  $1 \leq x \leq p^e$  and  $p \nmid x$  depends on the valuation  $v_p(n)$ .*

*When  $n$  is even, the number of solutions is*

$$\begin{cases} 2p^{e-2} & \text{if } 1 \leq e \leq 4 + v_p(n) \\ 2p^{\lfloor (e+v_p(n))/2 \rfloor} & \text{if } e \geq 5 + v_p(n). \end{cases}$$

*When  $n$  is odd, the number of solutions is*

$$\begin{cases} 2p^{e-2} & \text{if } 1 \leq e \leq 3 \\ p^{\lfloor e/2 \rfloor} + p & \text{if } e \geq 4. \end{cases}$$

REMARK 4. Note that in fact for even  $n$ , the formulas in the two cases above are equal if  $e = v_p(n) + 3$  or  $e = v_p(n) + 4$ , and when  $n$  is odd, the two cases are equal if  $e = 3$ .

#### 4. TWO-CYCLES

We now turn to the question of finding simultaneous roots of the functions  $x^{x^n} - y \pmod{p^e}$  and  $y^{y^n} - x \pmod{p^e}$ , where for a positive integer  $e$  and a prime  $p$ , we allow  $x, y \in \{1, 2, \dots, p^e(p-1)\}$  such that  $p \nmid x, p \nmid y$ . We again fix  $x_0, y_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$  and consider auxiliary functions  $\omega(x)^{g(x_0)} \langle x \rangle^{g(x)} - y \pmod{p^e}$  and  $\omega(y)^{g(y_0)} \langle y \rangle^{g(y)} - x \pmod{p^e}$  defined for a polynomial  $g$ .

We will use the isomorphism

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}/p^e\mathbb{Z})$$

induced from the decomposition (7) on  $\mathbb{Z}_p^\times$ . This isomorphism tells us that the two congruences

$$(13) \quad \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv y \pmod{p^e} \quad \text{and} \quad \omega(y)^{g(y_0)} \langle y \rangle^{g(y)} \equiv x \pmod{p^e}$$

are equivalent to the four equations

$$\begin{aligned} \langle x \rangle^{g(x)} &\equiv \langle y \rangle \pmod{p^e}, & \langle y \rangle^{g(y)} &\equiv \langle x \rangle \pmod{p^e}, \\ \omega(x)^{g(x_0)} &= \omega(y), & \text{and} & \quad \omega(y)^{g(y_0)} = \omega(x). \end{aligned}$$

Since  $x$  is completely determined by  $y$ , this is equivalent to solving the equations

$$\langle y \rangle^{g(x_{y_0}(y))g(y)} \equiv \langle y \rangle \pmod{p^e} \quad \text{and} \quad \omega(y)^{g(x_0)g(y_0)} = \omega(y),$$

or

$$(14) \quad \langle y \rangle^{g(x_{y_0}(y))g(y)-1} \equiv 1 \pmod{p^e} \quad \text{and} \quad \omega(y)^{g(x_0)g(y_0)-1} = 1,$$

where  $x_{y_0} : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  denotes the function

$$x_{y_0}(y) = \omega(y)^{g(y_0)} \langle y \rangle^{g(y)}.$$

**Theorem 13.** *Let  $p$  be a prime,  $p \neq 2$ , and  $g(x)$  be a polynomial. Then for every  $x_0, y_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , there are  $\gcd(p-1, g(x_0)g(y_0)-1)$  solutions  $(x, y)$  to the congruences*

$$(15) \quad \omega(x)^{g(x_0)} \langle x \rangle^{g(x)} \equiv y \pmod{p} \quad \text{and} \quad \omega(y)^{g(y_0)} \langle y \rangle^{g(y)} \equiv x \pmod{p}$$

where  $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ . Alternatively, for any given  $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ , there are

$$N_{G-1}(\text{ord}_p y) \left( \frac{p-1}{\text{ord}_p y} \right)^2$$

pairs  $(x_0, y_0) \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$  such that there exists an  $x \in (\mathbb{Z}/p\mathbb{Z})^\times$  which solves (15), where  $N_{G-1}(d)$  is the number of solutions to  $G(z_1, z_2) - 1 = g(z_1)g(z_2) - 1 \equiv 0$  modulo  $d$ . (Note that such an  $x$  is unique.)

*Proof.* The given congruences are equivalent to (14) with  $e = 1$ , which reduces to just

$$(16) \quad \omega(y)^{g(x_0)g(y_0)-1} = 1.$$

For fixed  $x_0$  and  $y_0$ , (16) is satisfied for exactly the  $y \in (\mathbb{Z}/p\mathbb{Z})^\times$  for which  $\text{ord}_p(y)$  divides  $g(x_0)g(y_0) - 1$ . There will be  $\gcd(p-1, g(x_0)g(y_0) - 1)$  such values for  $y$

in the cyclic group  $(\mathbb{Z}/p\mathbb{Z})^\times$ , and for each  $y$  there will be exactly one  $x$  in  $(\mathbb{Z}/p\mathbb{Z})^\times$  such that  $\omega(y)^{g(y_0)} \langle y \rangle^{g(y)} \equiv x \pmod{p}$ .

On the other hand, if  $y$  is fixed, then  $\text{ord}_p(y)$  divides  $g(x_0)g(y_0) - 1$  if and only if  $g(x_0)g(y_0) - 1 \equiv 0 \pmod{\text{ord}_p(y)}$ . There are  $N_{G-1}(\text{ord}_p y)$  such pairs  $(x_0, y_0)$  in  $(\mathbb{Z}/(\text{ord}_p y)\mathbb{Z})^2$  and  $N_{G-1}(\text{ord}_p y)((p-1)/\text{ord}_p y)^2$  such pairs in  $(\mathbb{Z}/(p-1)\mathbb{Z})^2$ . Once again, for each  $y$ ,  $x_0$ , and  $y_0$ , the equations prescribe a unique  $x$ .  $\square$

**Corollary 14.** *Let  $p$  be a prime,  $p \neq 2$ . Then there are*

$$\sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} \gcd(p-1, g(x_0)g(y_0)-1) = \sum_{d|p-1} \phi(d)((p-1)/d)^2 N_{G-1}(d)$$

*solutions  $(x, y)$  to the congruences*

$$x^{g(x)} \equiv y \pmod{p} \quad \text{and} \quad y^{g(y)} \equiv x \pmod{p}$$

*where  $1 \leq x, y \leq p(p-1)$  and  $p \nmid x, p \nmid y$ .*

*Proof.* The proof follows exactly the proof of Corollary 4.  $\square$

Next we consider  $p$ -adic solutions and solutions modulo  $p^e$ .

**DEFINITION 4.** Let  $T_{a,b,e}$  equal the set of solutions  $(x, y)$  to the equations

$$(17) \quad x^{g(x)} \equiv y \pmod{p^e} \quad \text{and} \quad y^{g(y)} \equiv x \pmod{p^e}$$

where  $1 \leq x, y \leq p^e(p-1)$  such that  $p \nmid x, p \nmid y$  and  $x \equiv a \pmod{p}, y \equiv b \pmod{p}$ .

This time, we will deal with three cases: where  $x^n y^n \not\equiv 1$  modulo  $p$ , where  $y^n \equiv x^{-n} \not\equiv -1$  modulo  $p$ , and where  $y^n \equiv x^n \equiv -1$  modulo  $p$ . For the first case, for which  $f_{y_0}(y)$  is nonsingular modulo  $p$ , we can deal with a more general polynomial  $g$ .

**Theorem 15.** *Let  $p$  be a prime,  $p \neq 2$ , and let  $a$  and  $b$  be such that  $g(a)g(b) \not\equiv 1$  modulo  $p$ . Then  $|T_{a,b,e}| = |T_{a,b,1}|$  for all  $e \geq 1$ .*

*Proof.* Fix  $y_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ . Let  $f_{y_0} : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  be the function

$$f_{y_0}(y) = \langle y \rangle^{g(x_{y_0}(y))g(y)-1} - 1.$$

Note that

$$\begin{aligned} f_{y_0}(y) &= \langle y \rangle^{g(x_{y_0}(y))g(y)-1} - 1 \\ &= \exp((g(x_{y_0}(y))g(y)-1) \log \langle y \rangle) - 1 \\ &= \left( 1 + (g(x_{y_0}(y))g(y)-1) \log \langle y \rangle + \frac{(g(x_{y_0}(y))g(y)-1)^2 (\log \langle y \rangle)^2}{2!} + \dots \right) - 1 \\ &= (g(x_{y_0}(y))g(y)-1) \log \langle y \rangle + \frac{(g(x_{y_0}(y))g(y)-1)^2 (\log \langle y \rangle)^2}{2!} + \dots \end{aligned}$$

Now  $\log \langle y \rangle \in p\mathbb{Z}_p$ , so

$$\begin{aligned} f'_{y_0}(y) &= \frac{d[g(x_{y_0}(y))g(y)-1]}{dy} \log \langle y \rangle + \frac{g(x_{y_0}(y))g(y)-1}{y} + (\text{terms containing } p) \\ f'_{y_0}(y) &\equiv \frac{g(x_{y_0}(y))g(y)-1}{y} \pmod{p}. \end{aligned}$$

Suppose we have  $x_1, y_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  such that  $g(x_1)g(y_1) \not\equiv 1 \pmod{p}$  and  $\omega(y_1)^{g(y_0)} \langle y_1 \rangle^{g(y_1)} \equiv x_1 \pmod{p}$ . Then  $x_{y_0}(y_1) \equiv x_1 \pmod{p}$ , and

$$f'_{y_0}(y_1) \equiv \frac{g(x_1)g(y_1) - 1}{y_1} \pmod{p}.$$

Since  $g(x_1)g(y_1) \not\equiv 1 \pmod{p}$  and  $y_1 \not\equiv 0 \pmod{p}$ , we have that  $f'_{y_0}(y_1) \not\equiv 0 \pmod{p}$ .

By Proposition 2, for fixed  $(x_0, y_0) \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$ , each solution  $y_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$  with  $g(x_{y_0}(y_1))g(y_1) \not\equiv 1 \pmod{p}$  to the equations

$$\langle y \rangle^{g(x_{y_0}(y))g(y)} \equiv 1 \pmod{p} \quad \text{and} \quad \omega(y)^{g(x_0)g(y_0)-1} = 1$$

will lift to a unique solution to

$$\langle y \rangle^{g(x_{y_0}(y))g(y)} = 1 \quad \text{and} \quad \omega(y)^{g(x_0)g(y_0)-1} = 1$$

in  $\mathbb{Z}_p$ . Thus this unique solution in  $\mathbb{Z}_p$  will correspond to one solution to equations (14), or equivalently (17), for each  $e$ . Applying the Chinese Remainder Theorem as before gives our result.  $\square$

Once again, we need to specialize to  $g(z) = z^n$  for the points  $y$  for which  $h_{y_0}(y)$  is singular modulo  $p$ .

**Theorem 16.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \nmid n$ , and let  $a, b \in \mathbb{Z}_p$  be roots of unity such that  $b^n = a^{-n}$ . Then*

$$|T_{a,b,e}| = \begin{cases} p^{\lfloor e/2 \rfloor} |T_{a,b,1}| & \text{if } b^n \neq -1 \\ p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} |T_{a,b,1}| & \text{if } b^n = -1 \end{cases}$$

for all  $e \geq 1$ .

*Proof.* Fix  $x_0, y_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , and consider  $y \equiv b \pmod{p}$  such that  $x_{y_0}(y) \equiv a \pmod{p}$ . Let  $h_{y_0}(y) = \log(\langle y \rangle^{x_{y_0}(y)^n y^{n-1}}) = (x_{y_0}(y)^n y^n - 1) \log \langle y \rangle$ , and note that  $h_{y_0}(y) \equiv 0 \pmod{p^e}$  is equivalent to  $f_{y_0}(y) \equiv 0 \pmod{p^e}$ , since  $z \mapsto \log(z+1)$  induces a bijection from  $p(\mathbb{Z}/p^e\mathbb{Z})$  to itself, fixing 0.

Let  $\bar{h}_{y_0}(y) = x_{y_0}(y)^n y^n$ , so  $h_{y_0}(y) = (\bar{h}_{y_0}(y) - 1) \log \langle y \rangle$ . Now

$$h'_{y_0}(y) = (\bar{h}_{y_0}(y) - 1)y^{-1} + \bar{h}'_{y_0}(y) \log \langle y \rangle,$$

$$h''_{y_0}(y) = -(\bar{h}_{y_0}(y) - 1)y^{-2} + 2\bar{h}'_{y_0}(y)y^{-1} + \bar{h}''_{y_0}(y) \log \langle y \rangle,$$

with

$$\bar{h}'_{y_0}(y) = \bar{h}_{y_0}(y)(n^2 y^{n-1} \log \langle y \rangle + n(y^n + 1)y^{-1}),$$

and

$$h'''_{y_0}(y) = 2(\bar{h}_{y_0}(y) - 1)y^{-3} - 3\bar{h}'_{y_0}(y)y^{-2} + 3\bar{h}''_{y_0}(y)y^{-1} + \bar{h}'''_{y_0}(y) \log \langle y \rangle$$

, with

$$\begin{aligned} \bar{h}''_{y_0}(y) &= \bar{h}'_{y_0}(y)(n^2 y^{n-1} \log \langle y \rangle + n(y^n + 1)y^{-1}) \\ &\quad + \bar{h}_{y_0}(y)(n^2(n-1)y^{n-2} \log \langle y \rangle + 2n^2 y^{n-2} - n(y^n + 1)y^{-2}). \end{aligned}$$

We will consider the Taylor series expansion for  $h_{y_0}(y)$  centered at  $y = b$ . Since  $b$  is a root of unity,  $\omega(b) = b$ , and  $\langle b \rangle = 1$ . Thus  $x_{y_0}(b) = \omega(b)^{y_0^n} \langle b \rangle^{b^n} = b^{y_0^n}$ . Since  $x_{y_0}(b) \equiv x_{y_0}(y) \equiv a \pmod{p}$ , the isomorphism (7) tells us that  $a = b^{y_0^n}$ , so  $x_{y_0}(b) = a$ ,  $\bar{h}_{y_0}(b) = a^n b^n = 1$ ,  $\bar{h}'_{y_0}(b) = n(b^n + 1)b^{-1}$ , and  $\bar{h}''_{y_0}(b) = n^2(b^n + 1)^2 b^{-2} +$

$2n^2b^{n-2} - n(b^n + 1)b^{-2}$ . Thus  $h_{y_0}(b) = 0$ ,  $h'_{y_0}(b) = 0$ ,  $h''_{y_0}(b) = 2n(b^n + 1)b^{-2}$ , and  $h'''_{y_0}(b) = -3n(b^n + 1)b^{-3} + 3\bar{h}''_{y_0}(b)$ .

The Taylor series expansion for  $h_{y_0}(y)$  centered at  $y = b$  is therefore

$$\begin{aligned} h_{y_0}(y) &= h_{y_0}(b) + h'_{y_0}(b)(y - b) + \frac{h''_{y_0}(b)}{2!}(y - b)^2 + \frac{h'''_{y_0}(b)}{3!}(y - b)^3 \\ &\quad + (\text{higher powers of } (y - b)) \\ &= 0 + 0(y - b) + n(b^n + 1)b^{-2}(y - b)^2 + (-n(b^n + 1)b^{-3} + \bar{h}''_{y_0}(b)b^{-1})(y - b)^3/2 \\ &\quad + (\text{higher powers of } (y - b)). \end{aligned}$$

If  $b^n \neq -1$ , then  $v_p(h_{y_0}(y)) = 2v_p(y - b)$ , and we proceed as in Theorem 7. Note that the number of solutions of  $h_{y_0}(y) \equiv 0 \pmod{p^e}$  is the same as the number of solutions of  $f_{y_0}(y) \equiv 0 \pmod{p^e}$  and that each solution to (14) again gives us a unique solution to (17) as in Theorem 15.

If  $b^n = -1$ , then

$$\begin{aligned} h_{y_0}(y) &= \bar{h}''_{y_0}(b)b^{-1}(y - b)^3/2 + (\text{higher powers of } (y - b)) \\ &= n^2b^{n-3}(y - b)^3 + (\text{higher powers of } (y - b)), \end{aligned}$$

and  $v_p(h_{y_0}(y)) = 3v_p(y - b)$ . An induction similar to Theorem 7 gives us the result stated in the theorem.  $\square$

**Theorem 17.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \nmid n$ . Then there are*

$$\begin{aligned} &\sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} \gcd(p-1, x_0^n y_0^n - 1) \\ &+ \sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} \gcd(p-1, n(y_0^n + 1), x_0^n y_0^n - 1) \cdot (p^{\lfloor e/2 \rfloor} - 1) \\ &+ \sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} (\gcd(p-1, 2n, x_0^n y_0^n - 1) - \gcd(p-1, n, x_0^n y_0^n - 1)) \cdot (p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} - p^{\lfloor e/2 \rfloor}) \\ &= \sum_{d|p-1} \phi(d)^2 \left( \frac{p-1}{d} \right)^2 N_{z^n-1}(d) \\ &+ \sum_{d|p-1} \phi(d) \left( \frac{p-1}{d} \right)^2 \mathcal{N}_{n(z^n+1)}(d) N_{z^n-1}(d) \cdot (p^{\lfloor e/2 \rfloor} - 1) \\ &+ \sum_{\substack{d|\gcd(p-1, 2n) \\ d \nmid \gcd(p-1, n)}} \phi(d)^2 \left( \frac{p-1}{d} \right)^2 N_{z^n-1}(d) \cdot (p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} - p^{\lfloor e/2 \rfloor}) \end{aligned}$$

solutions  $(x, y)$  to the congruences

$$x^{x^n} \equiv y \pmod{p^e} \quad \text{and} \quad y^{y^n} \equiv x \pmod{p^e}$$

where  $1 \leq x, y \leq p^e(p-1)$  such that  $p \nmid x$ ,  $p \nmid y$ ,  $N_{z^n-1}(d)$  is the number of solutions to  $z^n - 1 \equiv 0$  modulo  $d$ , and  $\mathcal{N}_{n(z^n+1)}(d)$  is the number of solutions to  $n(z^n + 1) \equiv 0$  modulo  $d$  such that  $z$  is relatively prime to  $d$ .

In particular, there are

$$\begin{aligned}
& \sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} \gcd(p-1, x_0 y_0 - 1) \\
& + \sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} \gcd(p-1, y_0 + 1, x_0 y_0 - 1) \cdot \left( p^{\lfloor e/2 \rfloor} - 1 \right) \\
& + \sum_{x_0=1}^{p-1} \sum_{y_0=1}^{p-1} (\gcd(2, x_0 y_0 - 1) - 1) \cdot \left( p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} - p^{\lfloor e/2 \rfloor} \right) \\
& = \sum_{d|p-1} \phi(d)^2 \left( \frac{p-1}{d} \right)^2 \\
& + \sum_{d|p-1} \phi(d) \left( \frac{p-1}{d} \right)^2 \cdot \left( p^{\lfloor e/2 \rfloor} - 1 \right) \\
& + \left( \frac{p-1}{2} \right)^2 \cdot \left( p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} - p^{\lfloor e/2 \rfloor} \right)
\end{aligned}$$

solutions  $(x, y)$  to the congruences

$$x^x \equiv y \pmod{p^e} \quad \text{and} \quad y^y \equiv x \pmod{p^e}$$

where  $1 \leq x, y \leq p^e(p-1)$  such that  $p \nmid x, p \nmid y$ .

*Proof.* The total number of solutions modulo  $p$  is given by Corollary 14. A solution  $(x, y)$  is in  $T_{a,b,1}$  as in Theorem 16 if and only if  $\omega(y)^{x_0^n y_0^n - 1} = 1$  and  $\omega(x)^n \omega(y)^n = \omega(y)^{n(y_0^n + 1)} = 1$ . (Note that  $\omega(x)$  and  $\omega(y)$  are roots of unity congruent modulo  $p$  to  $x$  and  $y$ , respectively.) This is equivalent to  $\omega(y)^{\gcd(n(y_0^n + 1), x_0^n y_0^n - 1)} = 1$ , and for a fixed  $x_0, y_0$  there are  $\gcd(p-1, n(y_0^n + 1), x_0^n y_0^n - 1)$  such  $y$ , each corresponding to a unique  $x$  modulo  $p$ . Alternatively, given a  $y \in (\mathbb{Z}/p\mathbb{Z})^\times$  of order  $d$ , there are

$$\left( \frac{p-1}{d} \right)^2 \left| \{ (x_0, y_0) \in (\{1, 2, \dots, d\})^2 \mid n(y_0^n + 1) \equiv 0 \pmod{d}, x_0^n y_0^n - 1 \equiv 0 \pmod{d} \} \right|$$

pairs  $(x_0, y_0) \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$  satisfying the conditions. There are  $\mathcal{N}_{n(z^n+1)}(d)$  values of  $y_0$  in the given set, and for each one there are  $N_{z^n-1}(d)$  values of  $x_0$ .

Furthermore, a solution  $(x, y)$  is in  $T_{a,b,1}$  as above with  $b^n = -1$  if and only if  $\omega(y)^{x_0^n y_0^n - 1} = 1$ ,  $\omega(x)^n = \omega(y)^{n(y_0^n)} = -1$ , and  $\omega(y)^n = -1$ . The third condition is equivalent to  $\omega(y)^{2n} = 1$  but  $\omega(y)^n \neq 1$ , and implies that the order of  $y$  must be even. Then the first condition implies that  $x_0^n y_0^n - 1$  must be even, so  $x_0$  and  $y_0$  must be odd, which combined with the third condition makes the second condition redundant. So we have  $\omega(y)^{x_0^n y_0^n - 1} = 1$ ,  $\omega(y)^{2n} = 1$ , and  $\omega(y)^n \neq 1$ , which is satisfied for  $\gcd(p-1, 2n, x_0^n y_0^n - 1) = \gcd(p-1, n, x_0^n y_0^n - 1)$  values of  $y$  for each fixed pair  $(x_0, y_0)$ . Alternatively, the conditions imply that for each  $y \in (\mathbb{Z}/p\mathbb{Z})^\times$  of order  $d$ ,  $d$  must divide  $2n$  but not  $n$ , and if so there are

$$\left( \frac{p-1}{d} \right)^2 \left| \{ (x_0, y_0) \in (\{1, 2, \dots, d\})^2 \mid x_0^n y_0^n - 1 \equiv 0 \pmod{d} \} \right|$$

pairs  $(x_0, y_0) \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$  satisfying the conditions. There are  $\phi(d)$  values of  $y_0$  in the given set, and for each one there are  $N_{z^n-1}(d)$  values of  $x_0$ .  $\square$



If  $p \mid n$ , the lifting of two-cycles that are singular modulo  $p$  again works the same as in Theorem 16 for large  $e$ , but all solutions lift for small  $e$ .

**Theorem 18.** *Let  $p$  be a prime,  $p \neq 2$  and  $p \mid n$ , and let  $a, b \in \mathbb{Z}_p$  be roots of unity such that  $b^n = a^{-n}$ . Then*

$$|T_{a,b,e}| = |T_{a,b,1}| \cdot \begin{cases} p^{e-1} & \text{if } e \leq v_p(n) \text{ and } b^n \neq -1 \\ p^{\lfloor (e+v_p(n))/2 \rfloor} & \text{if } e \geq v_p(n) + 1 \text{ and } b^n \neq -1 \\ p^{e-1} & \text{if } e \leq 2v_p(n) \text{ and } b^n = -1 \\ p^{\lfloor (e+v_p(n))/3 \rfloor + \lfloor (e+v_p(n)+1)/3 \rfloor} & \text{if } e \geq 2v_p(n) + 1 \text{ and } b^n = -1 \end{cases}$$

for all  $e \geq 1$ .

REMARK 5. Note that the powers of  $p$  in the first two formulas are the same as in Theorem 9, and the the second two formulas are equal if  $e = 2v_p(n) + 1$ ,  $e = 2v_p(n) + 2$ , or  $e = 2v_p(n) + 3$ .

*Proof.* As in the proof of Theorem 16, let  $x_0, y_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$ , and consider  $y \equiv b$  modulo  $p$  such that  $x_{y_0}(y) \equiv a$  modulo  $p$ . Let  $h_{y_0}(y) = (x_{y_0}(y)^n y^n - 1) \log \langle y \rangle = (\bar{h}_{y_0}(y) - 1) \log \langle y \rangle$ .

Note that  $\bar{h}'_{y_0}(y)$  is of the form  $n^2 \bar{U}(y) + n(y^n + 1) \bar{V}(y)$ , and  $h'_{y_0}(y)$  is of the form  $(\bar{h}_{y_0}(y) - 1)W(y) + n^2 U(y) + n(y^n + 1)V(y)$ . Induction then shows that  $h_{y_0}^{(i)}(y)$  will be of the same form for every  $i \geq 1$ .

If  $b^n \neq -1$ , then once again we have  $h_{y_0}(b) = h'_{y_0}(b) = 0$  and  $h''_{y_0}(b) = 2n(b^n + 1)b^{-2}$ . Since  $\bar{h}_{y_0}(b) = 1$ , we have  $h_{y_0}^{(i)}(b)$  divisible by  $n$  for every  $i \geq 2$ , and thus the Taylor series expansion for  $h_{y_0}(y)$  centered at  $y = b$  is

$$h_{y_0}(y) = n(b^n + 1)b^{-2}(y - b)^2 + n(\text{higher powers of } (y - b)).$$

Thus  $v_p(h_{y_0}(y)) = v_p(nb^{-1}(y - b)^2) = 2v_p(y - b) + v_p(n)$ . The proof in this case then proceeds exactly as in Theorem 9.

On the other hand, if  $b^n = -1$ , we have  $h_{y_0}(b) = h'_{y_0}(b) = h''_{y_0}(b) = 0$  and  $h'''_{y_0}(b) = 6n^2 b^{n-2}$ , and also  $h_{y_0}^{(i)}(b)$  is divisible by  $n^2$  for every  $i \geq 2$ . Thus the Taylor series expansion for  $h_{y_0}(y)$  centered at  $y = b$  is

$$h_{y_0}(y) = n^2 b^{n-2}(y - b)^3 + n^2(\text{higher powers of } (y - b)).$$

So  $v_p(h_{y_0}(y)) = v_p(n^2 b^{n-2}(y - b)^3) = 3v_p(y - b) + 2\ell$ , where  $\ell = v_p(n)$  as before.

Suppose  $1 \leq e \leq 3 + 2\ell$ . If  $h_{y_0}(b) \equiv 0$  modulo  $p$ , every  $y \equiv b$  modulo  $p$  is a solution to  $h_{y_0}(y) \equiv 0$  modulo  $p^e$ . This gives  $p^{e-1}$  solutions modulo  $p^e$  for every solution  $b$  modulo  $p$ . We then induct for  $e \geq 2\ell + 1$  as in Theorem 16, giving us  $p^{\lfloor (e-\ell)/3 \rfloor + \lfloor (e-\ell+1)/3 \rfloor} p^{2\ell} = p^{\lfloor (e+\ell)/3 \rfloor + \lfloor (e+\ell+1)/3 \rfloor}$  solutions modulo  $p^e$  for each solution modulo  $p$ . Applying the Chinese Remainder Theorem then gives us the result.  $\square$

A form of Theorem 17 then follows along the lines of Theorem 10.

When  $p = 2$ , we see that, as in the fixed point case, our equation is singular modulo  $p$  for all odd values of  $x$ . However, this time the lifting only takes two different forms, rather than three as in Theorem 11.

**Theorem 19.** *Let  $p = 2$ . Then when  $n$  is even and  $b = \pm 1$  or when  $n$  is odd and  $b = 1$ , we have that*

$$|T_{b,b,e}| = \begin{cases} p^{e-2} & \text{if } 2 \leq e \leq v_p(n) + 4 \\ p^{\lfloor (e+v_p(n)+1)/2 \rfloor} & \text{if } e \geq v_p(n) + 5 \end{cases}$$

for all  $e \geq 2$ . However, when  $n$  is odd and  $b = -1$ , we have that

$$|T_{b,b,e}| = \begin{cases} p^{e-2} & \text{if } 2 \leq e \leq 4 \\ p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} & \text{if } e \geq 5 \end{cases}$$

for all  $e \geq 2$ .

REMARK 6. Note that the powers of  $p$  in each of the two cases above are equal if  $e = v_p(n) + 4$  or  $e = v_p(n) + 5$ .

*Proof.* Consider  $y \equiv b \pmod{q}$ . Define  $h_{y_0}$  and  $\bar{h}_{y_0}$  as in the proofs of Theorems 16 and 18. Note that since  $p = 2$ ,  $y_0 = 1$ , and recall that the number of solutions to  $h_{y_0}(y) \equiv 0 \pmod{p^e}$  is the same as the number of solutions of  $f_{y_0}(y) \equiv 0 \pmod{p^e}$  and that each of these solutions gives us a unique two-cycle as in Theorem 15. As in the proof of Theorems 16 and 18, the Taylor series for  $h_{y_0}(y)$  centered at  $y = b$  is

$$\begin{aligned} h_{y_0}(y) &= h_{y_0}(b) + h'_{y_0}(b)(y-b) + \frac{h''_{y_0}(b)}{2!}(y-b)^2 + \frac{h'''_{y_0}(b)}{3!}(y-b)^3 \\ &\quad + (\text{higher powers of } (y-b)) \\ &= 0 + 0(y-b) + n(b^n + 1)b^{-2}(y-b)^2 + (-n(b^n + 1)b^{-3} + \bar{h}''_{y_0}(b)b^{-1})(y-b)^3/2 \\ &\quad + n(\text{higher powers of } (y-b)). \end{aligned}$$

Now we have two cases. First we consider the case where either  $b = \pm 1$  and  $n$  is even or where  $b = 1$  and  $n$  is odd, and second we will consider the case where  $b = -1$  and  $n$  is odd.

In our first case,  $b^{-2} = 1$ , and  $b^n + 1 = 2$ , so

$$h_{y_0}(y) = 2n(y-b)^2 + (n(\text{higher powers of } (y-b))).$$

Thus  $v_p(h_{y_0}(y)) = v_p(2n(y-b)^2) = 2v_p(y-b) + v_p(n) + 1$ .

Let  $\ell = v_p(n)$ . Suppose  $2 \leq e \leq \ell + 5$  and  $y$  satisfies  $1 \leq y \leq p^e$  and  $y \equiv b \pmod{q}$ . Note that since  $q = p^2$  and  $y \equiv b \pmod{q}$ ,  $v_p(y-b) \geq 2$ . Thus,

$$v_p(h_{y_0}(y)) = 2v_p(y-b) + v_p(n) + 1 \geq 4 + \ell + 1 = \ell + 5 \geq e,$$

so  $h_{y_0}(y) \equiv 0 \pmod{p^e}$ . There are  $p^{e-2}$  such values of  $y$  (recall that the coefficients of  $p^0$  and  $p^1$  are already determined), so there are  $p^{e-2}$  solutions to  $h_{y_0}(y) \equiv 0 \pmod{p^e}$ .

Now we induct on  $e$ , using  $e = \ell + 5$  as the base case. The preceding argument shows that there are  $p^{\ell+3}$  solutions to  $h_{y_0}(y) \equiv 0 \pmod{p^{\ell+5}}$ , and  $p^{\lfloor (\ell+5+\ell+1)/2 \rfloor} = p^{\lfloor (2\ell+6)/2 \rfloor} = p^{\ell+3}$ , so the base case agrees with the formula. The rest of the induction proceeds considering cases as in Theorem 7. Note that because  $v_p(h_{y_0}(y))$  is 1 larger than in the cases where  $p$  is odd (e.g., Theorem 9), a solution modulo  $p^e$  lifts to  $p$  solutions modulo  $p^{e+1}$  if  $e - \ell - 1$  is odd and one solution modulo  $p^{e+1}$  if  $e - \ell - 1$  is even.

However, in our second case where  $b = -1$  and  $n$  is odd, we have that  $b^{-2} = 1$ , and  $b^n + 1 = 0$ , so using our formulas for Theorem 16

$$\begin{aligned} h_{y_0}(y) &= 0 + 0(y-b) + 0(y-b)^2 - h''(b)(y-b)^3/2 + n(\text{higher powers of } (y-b)). \\ &= n^2(y-b)^3 + n(\text{higher powers of } (y-b)). \end{aligned}$$

Thus  $v_p(h_{y_0}(y)) = v_p(n^2(y-b)^3) = 3v_p(y-b)$ .

Suppose  $2 \leq e \leq 5$  and  $y$  satisfies  $1 \leq y \leq p^e$  and  $y \equiv b \pmod{q}$ . Note that as above,  $v_p(y-b) \geq 2$ . Thus,

$$v_p(h_{y_0}(y)) = 3v_p(y-b) \geq 6 > e,$$

so  $h_{y_0}(y) \equiv 0 \pmod{p^e}$  for all such  $y$ . There are  $p^{e-2}$  possible values of  $y$ , and all of them are solutions to  $h_{y_0}(y) \equiv 0 \pmod{p^e}$ .

Now we induct on  $e$ , using  $e = 5$  as the base case. The preceding argument shows that there are  $p^3$  solutions to  $h_{y_0}(y) \equiv 0 \pmod{p^5}$ , and  $p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} = p^3$ , so the base case agrees with the formula. The rest of the induction proceeds as in Theorem 16.  $\square$

**Corollary 20.** *Let  $p = 2$  and  $p \mid n$ . Then the number of solutions  $(x, y)$  to the congruences*

$$x^x \equiv y \pmod{p^e} \quad \text{and} \quad y^y \equiv x \pmod{p^e}$$

for  $1 \leq y \leq p^e$  where  $p \nmid y$  is

$$\begin{cases} 1 & \text{if } e = 1 \\ 2p^{e-2} & \text{if } 2 \leq e \leq v_p(n) + 4 \\ 2p^{\lfloor (e+v_p(n)+1)/2 \rfloor} & \text{if } e \geq v_p(n) + 5 \end{cases}$$

for all  $e \geq 1$ .

REMARK 7. Note that the formulas in each of the two cases above are equal if  $e = v_p(n) + 4$  or if  $e = v_p(n) + 5$ .

**Corollary 21.** *Let  $p = 2$  and  $p \nmid n$ . Then the number of solutions  $(x, y)$  to the congruences*

$$x^x \equiv y \pmod{p^e} \quad \text{and} \quad y^y \equiv x \pmod{p^e}$$

for  $1 \leq y \leq p^e$  where  $p \nmid y$  is

$$\begin{cases} 1 & \text{if } e = 1 \\ 2p^{e-2} & \text{if } 2 \leq e \leq 4 \\ p^{\lfloor (e+1)/2 \rfloor} + p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor} & \text{if } e \geq 5 \end{cases}$$

for all  $e \geq 1$ .

REMARK 8. Note that the formulas in each of the two cases above are equal if  $e = 4$  or if  $e = 5$ .

## 5. FUTURE WORK

Extending these results to cycles of size three and larger does not seem like it would present any theoretical difficulties. However, we expect that continuing our technique from Section 4 of reduction to one  $p$ -adic variable would result in such unwieldy formulas that the solution would not be worthwhile. Unfortunately, the multivariable technique used in [18, Section 5] only appears to apply to the cases that are nonsingular modulo  $p$ . A theory of lifting for points that are singular modulo  $p$  for multiple equations in multiple variables would be very useful here.

Another significant advance in the case of points that are singular modulo  $p$  would be to extend more of these results to the generalized self-power map  $x \mapsto x^{g(x)}$  for any polynomial  $g(x)$ . Our results can be used to count solutions modulo  $p$  for any polynomial. We can also determine which solutions are nonsingular modulo  $p$  and thus lift uniquely. On the other hand, we are not able to count the lifts that are singular modulo  $p$  without using a fairly specific form of the polynomial. Extending to  $g(x) = cx^n$  seems like a reasonable next case to try.

Two other types of congruences modulo  $p^e$  involving the self-power map were studied in [18], namely  $x^x \equiv c \pmod{p^e}$  and  $x^x \equiv y^y \pmod{p^e}$ . These could also be generalized to the expression  $x^{g(x)}$  studied here. In the case of  $x^x$ , these expressions are always nonsingular modulo  $p$ , but for some polynomials  $g(x)$ , this will no longer be the case.

This work explores solutions to our equations in the range  $\{1, \dots, p^e(p-1)\}$ . For cryptographic applications, we would be most interested in solutions in the range  $\{1, \dots, p^e\}$ . If  $p = 2$ , these are the same, and we find that we can both count and (by following the proofs) describe completely our solutions. For applications where we wish to take advantage of pseudorandom properties of functions, this suggests that variations on the self-power map may not be appropriate. It is possible that this predictability might be an advantage for other applications.

For  $p > 2$ , the standard heuristics suggest that the behavior modulo  $p-1$  of  $x \in \{1, \dots, p^e(p-1)\}$  is “independent” of the behavior modulo  $p^e$ . Thus, for example, if a fixed point  $x \in \{1, \dots, p^e(p-1)\}$  comes via the Chinese Remainder theorem from a pair  $(x_0, x_1) \in \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z}$ , we would expect approximately  $1/p$  of such fixed points to work out so that  $x \in \{1, \dots, p^e\}$ . (See, for example, [17] for similar heuristics.) This suggests that the numbers of fixed points and two-cycles in  $\{1, \dots, p^e\}$  should have some distribution centered around  $1/p$  times the numbers calculated in this paper. Some experimental results on this and related distributions in the case  $e = 1$  may be found in [11, Section 1.2; 12; 13, Section 8; 21, Section 4]. We are not aware of any similar results for  $e > 1$ .

## REFERENCES

- [1] Catalina Voichita Anghel, *The Self Power Map and its Image Modulo a Prime*, PhD Thesis, University of Toronto, 2013.
- [2] Catalina Anghel, *The self-power map and collecting all residue classes*, Mathematics of Computation **85** (2016), no. 297, 379–399, DOI 10.1090/mcom/2978.
- [3] Antal Balog, Kevin A. Broughan, and Igor E. Shparlinski, *On the Number of Solutions of Exponential Congruences*, Acta Arithmetica **148** (2011), no. 1, 93–103, DOI 10.4064/aa148-1-7.
- [4] Nicolas Bourbaki, *Commutative Algebra: Chapters 1-7*, 1st ed., Addison-Wesley, 1972.
- [5] Jan Camenisch and Markus Stadler, *Efficient group signature schemes for large groups*, Advances in Cryptology — CRYPTO ’97, 1997, pp. 410–424.

- [6] Jung Hee Cheon, *Discrete Logarithm Problems with Auxiliary Inputs*, Journal of Cryptology **23** (2009), no. 3, 457–476, DOI 10.1007/s00145-009-9047-0.
- [7] J. Cilleruelo and M. Z. Garaev, *Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications* (2014), available at [arXiv:1404.5070\[math\]](https://arxiv.org/abs/1404.5070).
- [8] Javier Cilleruelo and Mubbariz Z. Garaev, *On the congruence  $x^x \equiv \lambda \pmod{p}$*  (2015), available at [arXiv:1503.02730\[math\]](https://arxiv.org/abs/1503.02730).
- [9] Roger Crocker, *On a New Problem in Number Theory*, The American Mathematical Monthly **73** (1966), no. 4, 355–357.
- [10] ———, *On Residues of  $n^n$* , The American Mathematical Monthly **76** (1969), no. 9, 1028–1029.
- [11] Adam Tyler Felix and Pär Kurlberg, *On the fixed points of the map  $x \mapsto x^x$  modulo a prime, II* (2016), available at [arXiv:1607.04948\[math\]](https://arxiv.org/abs/1607.04948).
- [12] Matthew Friedrichsen and Joshua Holden, *Statistics for Fixed Points of the Self-power Map* (2014), available at [arXiv:1403.5548\[math\]](https://arxiv.org/abs/1403.5548).
- [13] Matthew Friedrichsen, Brian Larson, and Emily McDowell, *Structure and Statistics of the Self-Power Map*, Rose-Hulman Undergraduate Mathematics Journal **11** (2010), no. 2.
- [14] Fernando Quadros Gouvea,  *$p$ -adic Numbers: An Introduction*, 2nd ed., Springer, 1997.
- [15] Joshua Holden, *Fixed Points and Two-Cycles of the Discrete Logarithm*, Algorithmic number theory (ANTS 2002), 2002, pp. 405–415.
- [16] ———, *Addenda/corrigenda: Fixed Points and Two-Cycles of the Discrete Logarithm*, 2002. Unpublished, available at <http://xxx.lanl.gov/abs/math.NT/0208028>.
- [17] Joshua Holden and Pieter Moree, *Some Heuristics and Results for Small Cycles of the Discrete Logarithm*, Mathematics of Computation **75** (2006), no. 253, 419–449.
- [18] Joshua Holden and Margaret M. Robinson, *Counting Fixed Points, Two-Cycles, and Collisions of the Discrete Exponential Function using  $p$ -adic Methods*, Journal of the Australian Mathematical Society **92** (2012), 163–178.
- [19] Svetlana Katok,  *$p$ -adic Analysis Compared with Real*, American Mathematical Society, Providence R.I., 2007.
- [20] Neal Koblitz,  *$p$ -adic Numbers,  $p$ -adic Analysis, and Zeta-Functions*, 2nd, Graduate Texts in Mathematics, Springer, 1984.
- [21] Pär Kurlberg, Florian Luca, and Igor E. Shparlinski, *On the Fixed Points of the Map  $x \mapsto x^x$  Modulo a Prime*, Mathematical Research Letters **22** (2015), 141–168, DOI 10.4310/MRL.2015.v22.n1.a8.
- [22] Abigail Mann, *Counting Solutions to Discrete Non-Algebraic Equations Modulo Prime Powers*, Senior Thesis, Rose-Hulman Institute of Technology, 2016, [http://scholar.rose-hulman.edu/math\\_mstr/153](http://scholar.rose-hulman.edu/math_mstr/153).
- [23] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC, 1996.
- [24] Karen Reed, *Collisions of the Self-Power Map and Its Generalizations*, in preparation.
- [25] Lawrence Somer, *The Residues of  $n^n$  Modulo  $p$* , Fibonacci Quarterly **19** (1981), no. 2, 110–117.
- [26] Markus Stadler, *Publicly Verifiable Secret Sharing*, Advances in Cryptology — EUROCRYPT ’96, 1996, pp. 190–199.
- [27] L. Tóth, *Menon’s identity and arithmetical sums representing functions of several variables*, Rendiconti del Seminario Matematico. Università e Politecnico Torino **69** (2011), no. 1, 97–110.
- [28] A. Wood, *The Square Discrete Exponentiation Map*, Technical Report MSTR 11-05, Mathematical Sciences Technical Reports, Rose-Hulman Institute of Technology, 2011, [http://scholar.rose-hulman.edu/math\\_mstr/9/](http://scholar.rose-hulman.edu/math_mstr/9/).

DEPARTMENT OF MATHEMATICS, ROSE-HULMAN INSTITUTE OF TECHNOLOGY, 5500 WABASH  
AVE., TERRE HAUTE, IN 47803, USA

*E-mail address:* `holden@rose-hulman.edu`

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, WESTMINSTER COLLEGE, 319 SOUTH  
MARKET STREET, NEW WILMINGTON, PA 16172, USA

*E-mail address:* `richarpa@westminister.edu`

DEPARTMENT OF MATHEMATICS AND STATISTICS, MOUNT HOLYOKE COLLEGE, 50 COLLEGE  
STREET, SOUTH HADLEY, MA 01075, USA

*E-mail address:* `robinson@mtholyoke.edu`